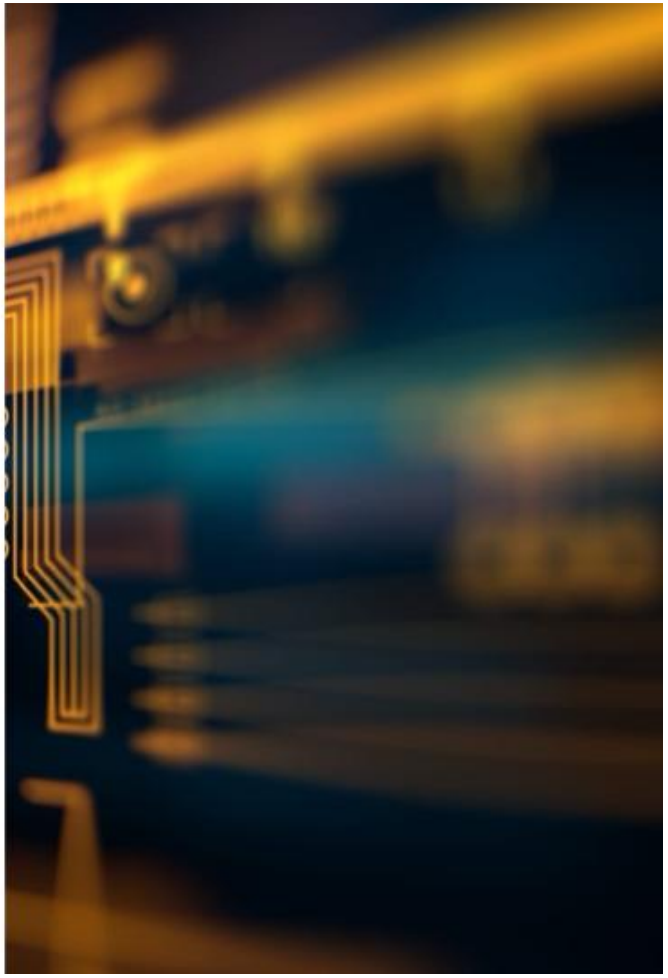
ASSESSING THE READINESS OF CARIBBEAN BOARDS FOR EFFECTIVE CYBERSECURITY OVERSIGHT

By: Ron Sookram

Arthur Lok Jack Global School of Business

January 2025

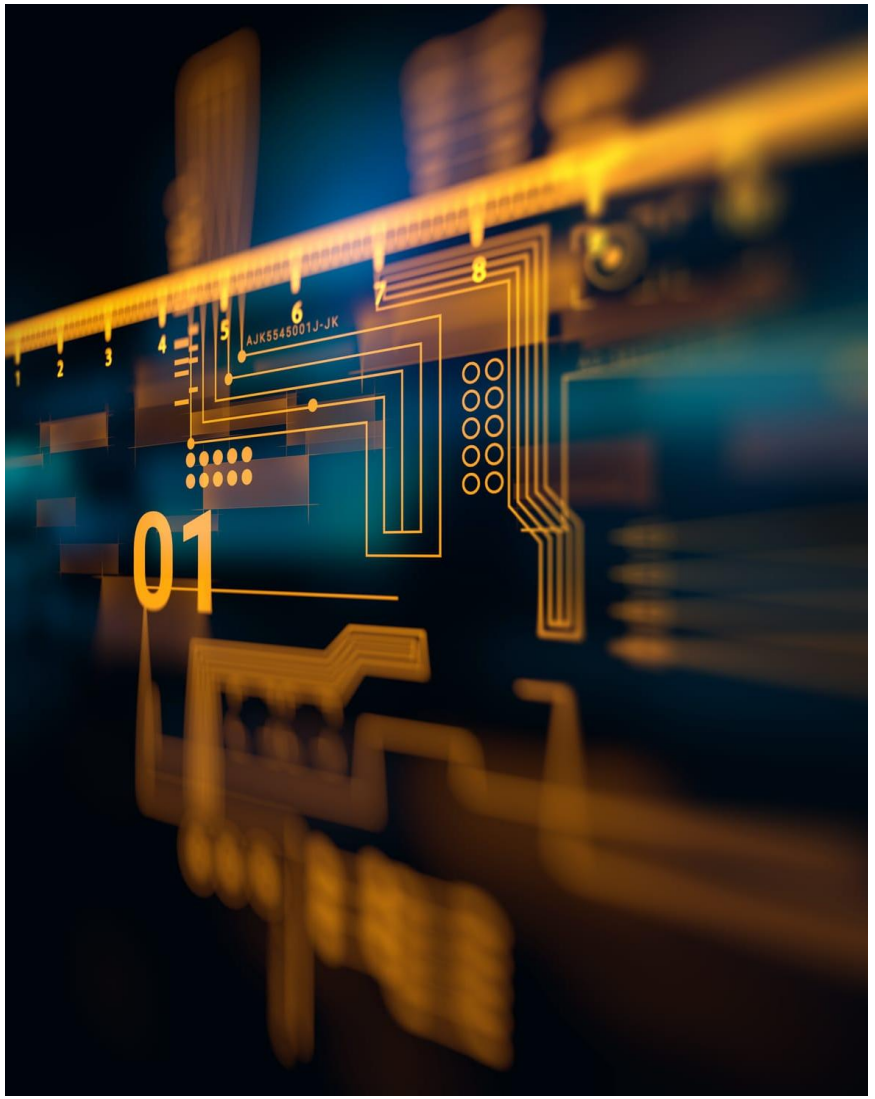


CONTENTS

INTRODUCTION

In today's interconnected digital landscape, cyber-attacks have become critical concerns for organizations worldwide. These attacks have grown in both scale and sophistication, presenting significant risks to an organization's assets, operations, and reputation. Consequently, for boards of directors, ensuring robust cybersecurity oversight is no longer optional—it is a fundamental aspect of strategic risk management. However, the readiness of boards to provide effective governance over these risks remains a pressing issue, especially in the Caribbean. Here, challenges such as limited resources, varying expertise levels, and inconsistent governance practices pose additional hurdles to achieving robust cybersecurity oversight.

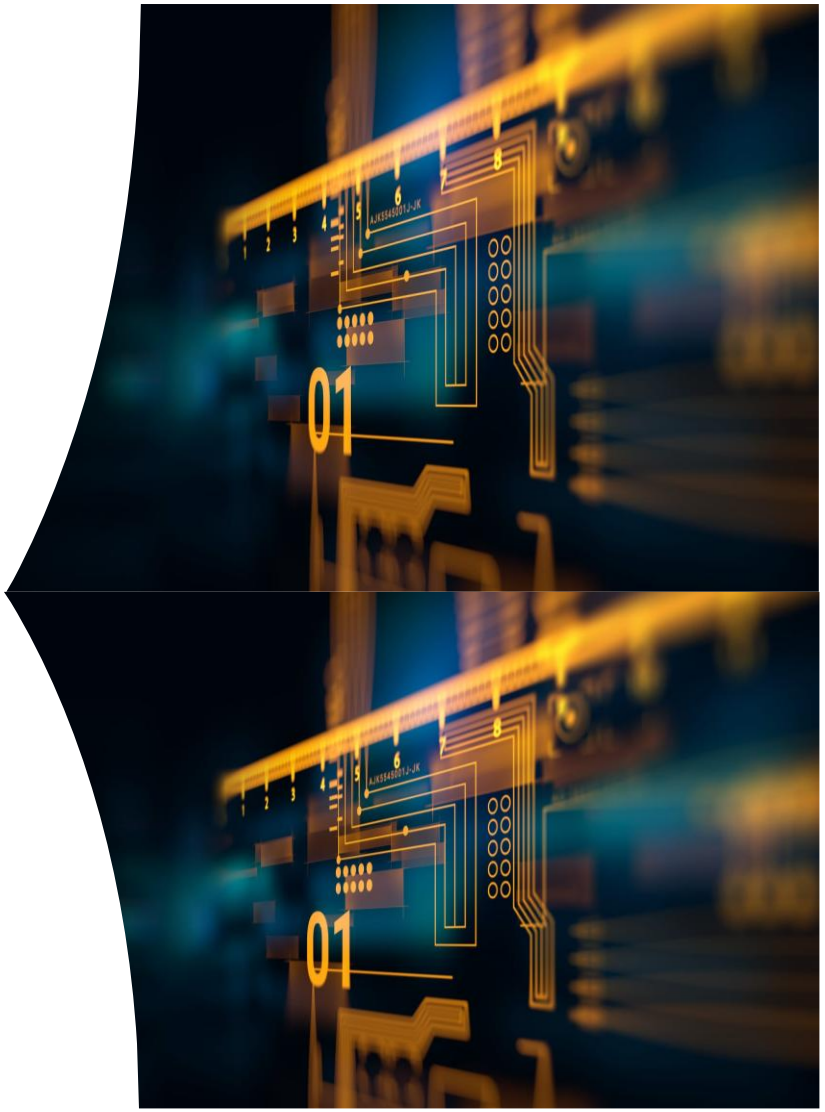
This study aims to assess the current state of board-level cybersecurity governance among Caribbean organizations by examining key areas such as the understanding of cybersecurity risks, reporting practices, funding, and expertise. The research identifies critical gaps that hinder effective oversight. The findings provide actionable insights and recommendations to help boards enhance their governance frameworks, build resilience against cyber threats, and align with global best practices. In doing so, this study contributes to the broader discourse on strengthening cybersecurity governance within the unique context of the Caribbean.



EXECUTIVE SUMMARY

This report examines the state of board-level cybersecurity governance across the Caribbean, uncovering critical gaps and challenges in cybersecurity oversight.

It offers actionable recommendations aimed at strengthening governance frameworks, improving oversight capabilities, and effectively addressing these challenges to enhance organizational resilience.



EXECUTIVE SUMMARY: KEY FINDINGS

- **Cybersecurity Audits:** Most organizations have conducted cybersecurity audits.
- **Cybersecurity Insurance:** Many have not considered cyber insurance, reflecting a limited focus on risk transfer strategies.
- **Insufficient Understanding of Cybersecurity Risk**: Few directors rated their boards' understanding of cybersecurity as excellent. Significant gaps remain, particularly in managing technology and data privacy risks.
- **Inconsistent Cybersecurity Reporting**: Boards Lack Regular Updates on Cybersecurity.
- **Prioritized Practices**: Organizations emphasize identifying critical assets, conducting risk assessments, and testing data backups.
- **Limited Funding:** Many directors expressed dissatisfaction with cybersecurity funding.
- **Difficulty in Finding Relevant Expertise**: Limited board appointments of directors with cybersecurity expertise, leading to reliance on external consultants and upskilling initiatives

EXECUTIVE SUMMARY: KEY FINDINGS

Caribbean boards face four primary challenges in governing cybersecurity:

1. **Resource Constraints**: Limited financial resources delay cybersecurity investments and preparedness.
2. **Shortage of Experts:** A regional shortage of cybersecurity professionals limits board access to specialized expertise.
3. **Narrow Perspectives:** Some boards view cybersecurity as an IT issue rather than a strategic priority.
4. **Focus on Short-Term Goals:** Volatile Caribbean markets drive boards to prioritize immediate business performance over long-term cybersecurity strategies.

Actionable Steps that can be taken:

1. **Prioritize Cybersecurity** as a Strategic Issue, Not Just an IT Concern
2. **Enhance Cybersecurity Expertise** through recruitment and selection or staffing upskilling
3. **Allocate Sufficient Resources** for Cybersecurity Investments
4. **Make Cybersecurity a Responsibility** of the Audit or Risk Management Committee
5. **Conduct Regular** Cybersecurity Audits and Risk Assessments
6. **Develop and Test** a Cybersecurity Incident Response Plan

These and other recommendations are discussed in the report**.**

TYPES OF CYBER-ATTACKS & THEIR IMPACT ON ORGANIZATIONS

For this study, the information on various types of cyberattacks is sourced from Fortinet, a global leader in cybersecurity solutions and services. According to Fortinet, a cyberattack is an action aimed at compromising a computer or any component of a digital information system with the intent to alter, destroy, or steal data, or to exploit and damage networks.

- **Malware and Ransomware**

Among the most prevalent types of cyberattacks are malware and ransomware, which infiltrate systems to steal, corrupt, or destroy confidential information. **Malware** encompasses various forms, including viruses, Trojan horses, worms, and spyware, each designed to exploit computer functions. Malware can cause extensive harm, such as

- Deleting files
- Collecting personal information and sharing it with unauthorized third parties
- Recording keystrokes and enabling unauthorized access to webcams
- Using a compromised computer to hack other systems
- Disabling security settings
- Sending spam emails
- Hijacking web browsers

Ransomware is a type of malware that restricts users from accessing their computers and demands payment in exchange for restoring functionality. Despite the emergence of new threats, it continues to be a prevalent form of cyberattack.

Other types of Cyberattacks include, but are not limited to:

- **Phishing and Spear-Phishing Scams** - hackers send authentic-looking emails and text messages to their targets to steal personal and financial information. The messages often ask victims to update, validate or confirm accounts.
- **Password Attacks/Brute-Force Logins** – Hackers attempt to figure out passwords or encryption keys to gain access to databases, accounts and other sensitive digital spaces.
- **Denial of Service (DoS)/Distributed Denial of Service (DDoS) -** often used against large companies and organizations. Their point is to shut down the system or website in question. The hackers exploit one system vulnerability and use it to send massive quantities of data to the rest of the network, until the system is so inundated that it becomes extremely slow or unable to function at all.
- **Man-in-the-Middle (MITM)** – Hackers impersonate end users to obtain sensitive information.
- **Advanced Persistent Threat (APT)-** stealthy infiltrations that seek to obtain information from a network over a long period, typically months or years.
- **Server-Side Request Forgery (SSRF)** – hacker exploits a vulnerable web application and then deceives it into redirecting malicious requests to the internal network or local host behind the system firewall — thus bypassing the network's defenses.

IMPACT ON ORGANIZATIONS

A successful cyberattack can inflict significant harm on organizations, affecting their financial performance, reputation, and consumer trust. The consequences of a security breach typically fall into three key categories: financial, reputational, and legal.

- **Financial cost:** Cyberattacks often lead to significant financial losses, which may arise from:

- ⇒ Theft of corporate information
- ⇒ Theft of financial details (e.g., bank or payment card information)
- ⇒ Direct theft of funds
- ⇒ Disruption to operations (e.g., inability to conduct online transactions)
- ⇒ Loss of business or contracts
- ⇒ Increased cybersecurity insurance premiums

Statista
In 2024, the average cost of an industrial data breach was US$5.56 million, up from US$4.73 million in 2023.

Additionally, businesses typically face expenses related to addressing the breach, including repairing compromised systems, networks, and devices.

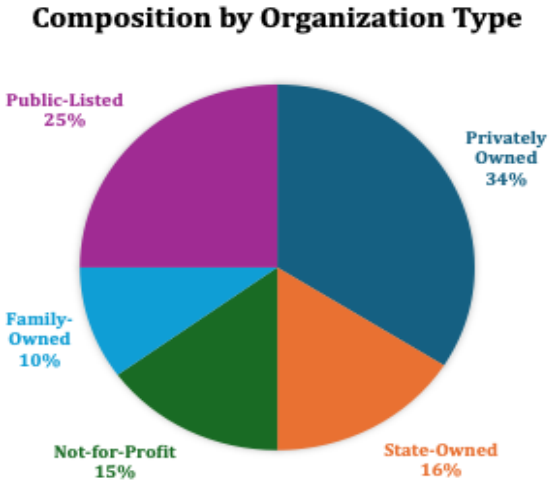
- **Reputational damage:** Trust is a cornerstone of customer relationships. Cyberattacks can severely damage a business's reputation and undermine customer confidence, leading to significant consequences such as:
  - ⇒ Loss of customers
  - ⇒ Decline in sales
  - ⇒ Reduction in profits

  The repercussions of reputational damage can extend beyond customers, affecting relationships with suppliers, partners, investors, and other third parties who have a vested interest in the business.

- **Legal consequences of a cyber breach:** Data protection and privacy regulations mandate that companies safeguard all personal data in their possession, whether it pertains to employees or customers. Failure to implement adequate security measures could result in the accidental or intentional compromise of this data. In such cases, organizations may be subject to significant fines and regulatory penalties, depending on the laws in force within their jurisdictions.

METHODOLOGY

The data for this report was gathered through a survey distributed to 150 directors across the Caribbean. The survey achieved a 70% response rate, with 105 completed responses. The survey instrument was disseminated via the Corporate Governance Institute of the Caribbean (CCGI) network and other professional and business networks to ensure broad participation.



4

Main Findings

How prepared are Caribbean Boards to effectively oversee cybersecurity risks and strategies?

OVERVIEW OF THE CARIBBEAN CYBERSECURITY LANDSCAPE

The Caribbean region has one of the highest internet usage rates globally

High Internet Usage Rates

- 67.4 percent of the Caribbean population online in 2020, surpassing the global average of 52.4 percent.
- This high level of connectivity has driven significant digital transformation, which was further accelerated by the COVID-19 pandemic, spurring technology adoption, digitalization, and automation across business, industry, and services.

Increased Cyber Threat Vulnerability

- There is a surge in cybercriminal activity targeting internet-connected and cloud-based systems.
- In the first six months of 2022, 144 million attempted cyberattacks occurred in the region, with ransomware being the most common breach.

Increasing Cyber-attacks in the Region

Recent Cybersecurity Incidents 2023

- **Bermuda**: Government IT systems disrupted.
- **Jamaica**: Financial Services Commission targeted by ransomware.
- **Belize**: Confidential data breach at Belize Electricity Limited.
- **Trinidad and Tobago**:
  - 205 successful cyberattacks reported to TT-CSIRT (2019-2024).
  - 52 incidents occurred in 2023.

Notable Cyber Attacks

- **2023**: Telecommunications Services of Trinidad and Tobago (TSTT) experienced a cyber breach
- **2023**: National Insurance Board of Trinidad and Tobago (NIBTT) faced a ransomware attack
- **2022**: Massy Stores & Massy Distribution in Jamaica and Trinidad targeted by Hive Ransomware. 17GB of sensitive data leaked after ransom refusal.
- **2020**: Ansa McAl was attacked by REvil Cyberberg. 12.9GB of data leaked after the company declined to pay a ransom

Cyberattacks are growing in frequency and sophistication.

- Boards must prioritize cybersecurity readiness and resilience strategies.
- Effective oversight is critical to safeguarding organizations from escalating cyber threats.

Cybersecurity Audits & Insurance

Most organizations have conducted cybersecurity audits to evaluate and strengthen their systems.

- However, 56% of directors reported that cyber insurance had not been considered, highlighting a limited focus on risk transfer strategies.
- Directors' views on cyber risk responsibility varied, with 60% assigning it to management, 41% to the board, and 28% uncertain.

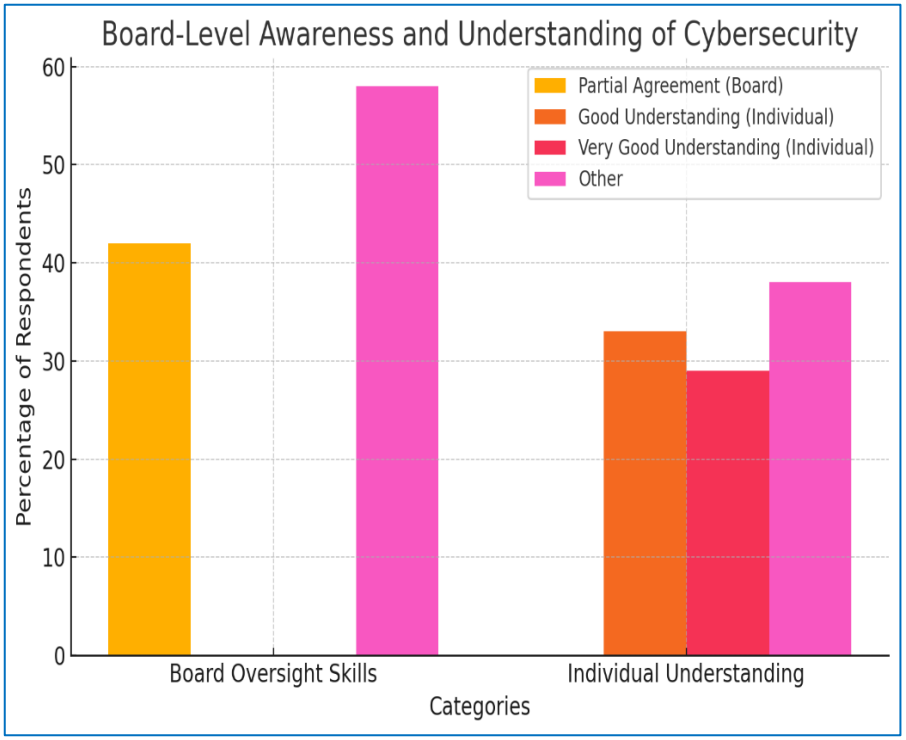
Gaps in Oversight Skills and Awareness

Gaps in Oversight Skills

- 42% of directors *partially agreed* that their boards possess the necessary cybersecurity oversight skills.
- The majority highlighted a lack of essential competencies in managing technology and data privacy risks.

Individual Competence

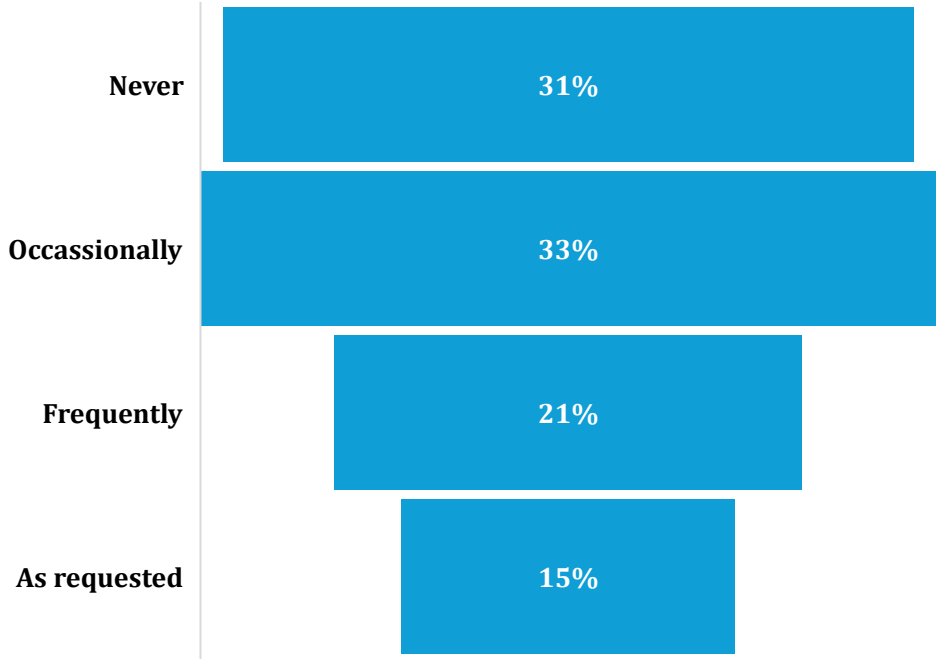
- 33% of directors rated their personal understanding of cybersecurity as **good**.
- 29% rated their understanding as **very good**



Inconsistency in Cybersecurity Reporting

- 31% of boards never received reports on cybersecurity issues
- 33% of directors reported occasional updates from management
- Only 21% confirmed frequent Cybersecurity reporting

How Often does your board receive reports on Cyber-related issues?

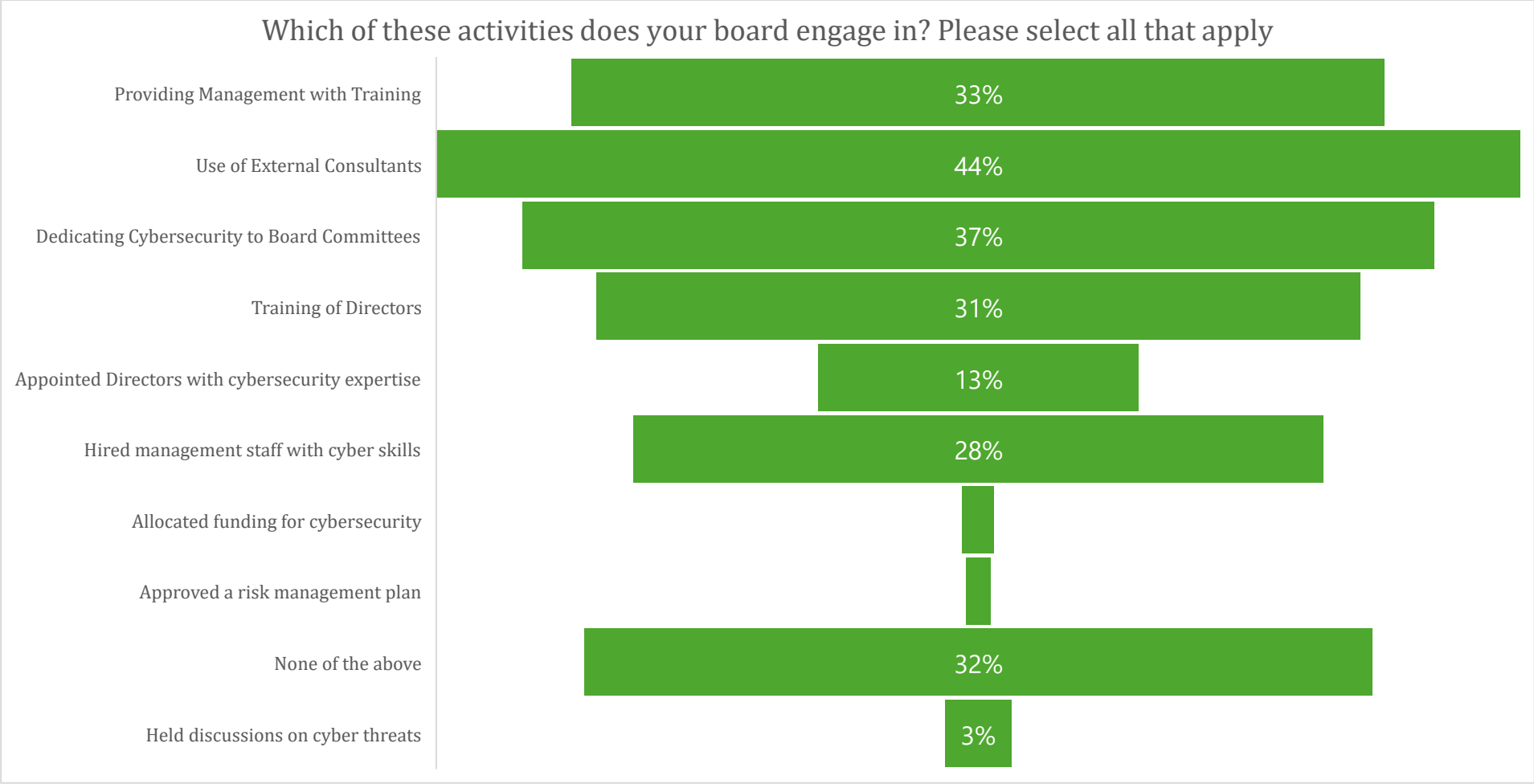


Top Cybersecurity Practices

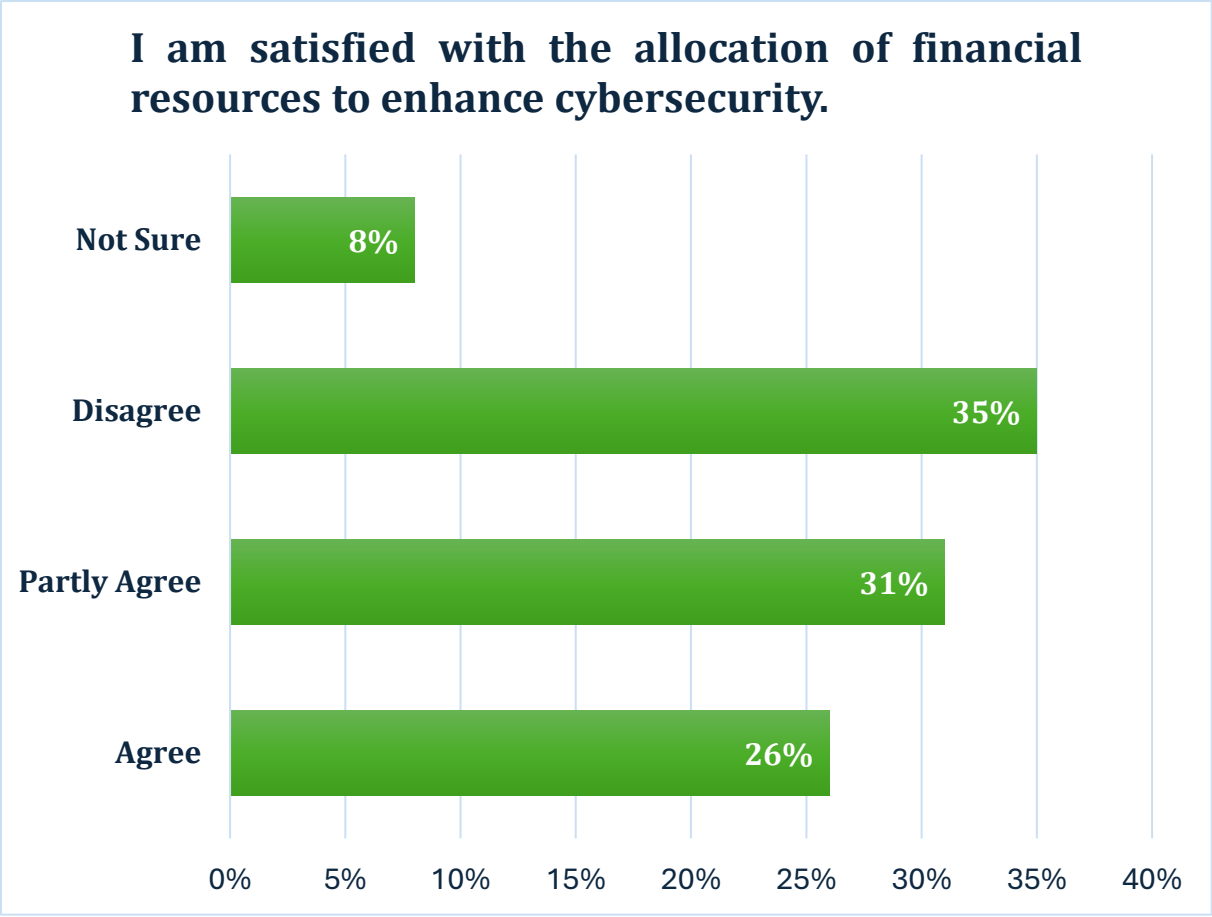
Key practices prioritized by organizations include:

1. Identifying critical assets and processes
2. Conducting risk assessments
3. Regular testing of data backups, and
4. Communicating cybersecurity strategies with staff training

Boards' Cybersecurity Activities



Investments in Cybersecurity



Financial resources allocated to Cybersecurity need to increase. Directors are not satisfied with the current level of funding.

CHALLENGES IN BOARD-LEVEL CYBERSECURITY OVERSIGHT

- **Limited Understating of Cybersecurity**: Only 16% of directors reported that their boards had a strong grasp of cybersecurity's strategic importance. This lack of awareness often leads to cybersecurity being viewed as merely an "IT issue" with low urgency, causing boards to underestimate the significant organizational risks posed by cyber threats. With this limited perspective, boards may assume that cyberattacks are primarily focused on stealing information, overlooking the more severe threats of operational disruptions or ransomware attacks that could cripple the organization.

- **Resource Limitations**: Directors frequently cited limited financial resources as a primary barrier to improving cybersecurity. The high costs associated with acquiring necessary assets and services often delay organizations' cybersecurity preparedness.

- **Shortage of Cybersecurity Experts**: The Caribbean has a limited pool of cybersecurity professionals, making it challenging for boards to appoint directors with the requisite expertise. When such skills are available, they come at a premium, and qualified professionals are often overextended, serving multiple organizations. As a result, boards may struggle to secure the cybersecurity expertise they need, even when they acknowledge its necessity

- **Focus on Immediate Business Priorities**: In the face of volatile markets, many boards prioritize short-term performance over long-term strategic goals, including cybersecurity. While boards recognize the potential for cyberattacks, there is a tendency to defer action, assuming that cyber risks can be managed once more immediate challenges have been addressed.

SUMMARY OF FINDINGS

1. **Cybersecurity Knowledge and Risk Management**:

   - Significant gap between recognizing cybersecurity needs and understanding risk management, especially cyber insurance.
   - Boards often overlook the strategic value of risk transfer.

2. **Board-Level Skills and Training**:

   - Low ratings for board-level oversight and understanding highlight the need for education and training.
   - Directors feel personally competent but recognize collective gaps in their boards' cybersecurity capabilities.

3. **Inconsistent Reporting and a focus on operational oversight:**

   - The lack of regular cybersecurity reporting stems from low prioritization and awareness among directors.
   - Operational efforts (e.g., risk assessments, and data backups) lack alignment with strategic governance frameworks.

4. **Challenges in Cybersecurity Funding and Expertise:**

   - Funding limitations impede advanced cybersecurity measures.
   - Few boards appoint directors with specialized cybersecurity expertise.
   - Engaging consultants and management training have shown progress but are insufficient.

COMPARING GLOBAL CYBERSECURITY DEVELOPMENTS

- **Recognition of Cybersecurity as a Strategic Priority:** Cybersecurity has evolved from being seen solely as an IT issue to a central aspect of enterprise-wide risk management.

- **Regulatory Influence and Accountability:** Regulatory developments have significantly increased board accountability for cybersecurity. For example, The US SEC's requirements for board-level cybersecurity expertise and mandatory disclosure illustrate the growing regulatory expectations. Similarly, the EU's NIS2 directive further reinforces this, imposing personal liability on board members for cybersecurity failures, thereby strengthening their role in maintaining cybersecurity standards

- **Availability of Board Expertise in Cybersecurity:** Global trends highlight the need for board members with specialized cybersecurity expertise to ensure informed oversight and decision-making. Many organizations are encouraged, or even required, to include directors with cybersecurity experience on their boards

- **Emphasis on Resilience and Recovery:** Globally, there is an increasing focus on organizational resilience and recovery within cybersecurity governance. Regulatory standards and best practices now advocate for boards to consider not only preventive measures but also strategies for recovering from cyber incidents.

- **Cybersecurity Culture and "Tone at the Top":** Globally, boards are encouraged to set a "tone at the top" that fosters a cybersecurity-conscious culture throughout the organization. This cultural shift helps position cybersecurity as a shared responsibility across all levels of the organization, supported by continuous board engagement and integration into the overall business strategy

- **Management of Third-Party and Geopolitical Risks:** Given the interconnected nature of cybersecurity risks, global boards increasingly focus on managing third-party and geopolitical risks. This includes evaluating cyber risks posed by suppliers, partners, and vendors, as well as considering geopolitical factors that might affect data

sovereignty and supply chain security. These considerations are becoming integral to global cybersecurity governance.

Comparing Global Cybersecurity Developments

- A significant gap exists between global cybersecurity governance standards and the practices observed among Caribbean boards. Globally, while boards are increasingly focused on accountability, expertise, resilience, and fostering a proactive cybersecurity culture, Caribbean boards are still in the early stages of integrating these elements into their governance frameworks.

- Factors such as the lack of regulatory requirements, limited board expertise, and a focus on preventive rather than resilience-oriented strategies contribute to this discrepancy.

- Caribbean boards could benefit from regulatory support, enhanced board training, and a strategic shift towards comprehensive cybersecurity governance to close this gap. By addressing these areas, Caribbean boards can strengthen their readiness and resilience against cyber threats, better protecting their organizations in an increasingly digital world.

SPOTLIGHT

Caribbean boards demonstrate a limited understanding of cybersecurity, often viewing it as a purely technical issue rather than an operational and strategic business risk. This perspective hinders effective governance, leaving organizations vulnerable to evolving cyber threats.

Enhanced board-level education and training are crucial to bridge this knowledge gap and foster a more strategic approach to managing cybersecurity risks.


01
Recommendations
Action Ideas for Boards

1. Prioritize Cybersecurity as a Strategic Issue, Not Just an IT Concern

- Boards should reframe cybersecurity as a critical strategic and risk management issue, integrating it into the broader corporate governance framework. This shift in perspective elevates cybersecurity to a priority level, encouraging a proactive stance beyond a purely technical issue.
- Board charters should be updated to explicitly include cybersecurity oversight responsibilities, and cyber risk discussions should become a standing agenda item in all board meetings

2. Enhance Cybersecurity Expertise

- Boards should prioritize the recruitment of directors with cybersecurity expertise or provide targeted cybersecurity training to individual members with relevant backgrounds and interests.
- Engaging consultants to provide regular cybersecurity training sessions for all board members.
- At the management level, boards can ensure the selection, recruitment, or upskilling of individuals to strengthen the organization's cybersecurity capabilities. With enhanced expertise, boards will be better positioned to oversee and align cybersecurity strategies with organizational objectives and regulatory requirements

3. Make Cybersecurity a Responsibility of the Audit or Risk Management Committee

- To ensure a sustained focus on cybersecurity, it is recommended that boards assign cybersecurity oversight to a dedicated standing committee, such as the audit or risk management committee. This structure provides the necessary accountability and focus on cybersecurity, ensuring that evolving cyber threats and recovery responses are continuously monitored.

4. Implement Consistent and Structured Cybersecurity Reporting

- Boards should establish a standardized reporting framework for cybersecurity, ensuring regular updates on key metrics such as incident response times, risk assessments, and compliance statuses.
- These reports should be provided at clear intervals (e.g., quarterly or bi-annually), ensuring that boards have timely and relevant information to make informed decisions.
- The reports should cover internal training, incident response, third-party risk, and other key cybersecurity initiatives.

5. Invest in Cyber Insurance and Develop a Risk Transfer Strategy

- Boards should evaluate the role of cyber insurance as part of a comprehensive risk management strategy. Cyber insurance can serve as a financial safeguard, mitigating the financial impact of a significant cyber incident.
- Boards should engage risk management professionals to assess their organization's cyber insurance needs and determine the appropriate coverage, including limits, exclusions, and scope of coverage

6. Conduct Regular Cybersecurity Audits and Risk Assessments

- Schedule regular cybersecurity audits and risk assessments to identify vulnerabilities, monitor compliance with cybersecurity policies, and evaluate the effectiveness of security measures.
- These assessments will help boards detect vulnerabilities early and ensure their cybersecurity strategies remain aligned with the evolving threat landscape

7. Develop and Test a Cybersecurity Incident Response Plan

- Establishing a comprehensive incident response plan is essential for quick and coordinated action in the event of a cyber incident. The plan should include clear communication protocols, mitigation strategies, and recovery procedures.
- Regular simulations or tabletop exercises involving board members will enhance readiness and ensure that the organization is prepared to minimize the impact of cyber incidents.

8. Leverage External Consultants to Address Expertise Shortages

- Where direct cybersecurity expertise is lacking, boards should engage external consultants to provide guidance, conduct assessments, and assist in the development of governance frameworks.
- External consultants offer a cost-effective solution for organizations with limited in-house resources, providing specialized expertise to enhance cybersecurity governance.

9. Allocate Sufficient Resources for Cybersecurity Investments

- Boards must commit to adequate financial resources for cybersecurity infrastructure, training, and initiatives, ensuring they are aligned with emerging threats and industry benchmarks.
- Regular reviews of the cybersecurity budget, alongside benchmarking against industry standards, will help prioritize cyber risk. These reviews should be conducted annually to adjust resource allocations and ensure that cybersecurity investments remain competitive and robust.

CONCLUSION

The findings of this study reveal that Caribbean boards face significant challenges in providing effective cybersecurity oversight. Limited understanding of cybersecurity risks, inconsistent reporting practices, and a lack of specialized expertise hinder their ability to address emerging cyber threats strategically. While operational measures such as threat assessments and data backups are in place, they lack alignment with broader governance frameworks. Furthermore, inadequate funding and reliance on external consultants underscore the need for a more proactive approach to building internal capacity.

To enhance their preparedness, Caribbean boards must prioritize cybersecurity as a strategic imperative. This includes investing in board-level training, recruiting directors with specialized expertise, and establishing structured reporting mechanisms. By adopting a forward-looking and comprehensive governance approach, boards can strengthen their oversight capabilities, safeguard critical assets, and bolster organizational resilience against the growing threat of cyberattacks. Ultimately, addressing these gaps will position Caribbean boards to align with international best practices and build trust with stakeholders in an increasingly digital world.

Dr. Ron Sookram
Academic Director & Team Lead- Corporate Governance Services
r.sookram@lokjackgsb.edu.tt